Security on the Cloud

Steven H. Dam, Ph.D., ESEP, President, SPEC Innovations, **Chris Ritter, Daniel Hettema**
571-485-7805
steven.dam@specinnovations.com

October 2013

Overview

- How Secure Is Your Network?
- What is Cloud Computing?
- What Are the Key Security Issues?
- What is FedRAMP?
- How Are We Trying to Fix the Problem?
- What Does Google Do?
- Summary

SPEC INNOVATIONS

How Secure Is Your Network?

"For the better part of a decade, I have worked to raise awareness of the growing threat from cyberattacks from countries like China, which steal critical information from both the government and the private sector." Congressman Frank Wolf, Chairman of the House Appropriations Subcommittee on Commerce, Justice, and Science

– from http://wolf.house.gov/cybersecurity accessed 9/23/2013

"Fallout from a breach at EMC Corp.'s RSA Security division earlier this year continues to cascade through the defense industry, as information taken in that breach is believed to have been used against major contractor L-3 Communications Holdings Inc. The report follows a similar attack against contracting giant Lockheed Martin."

– from "Another major defense contractor hacked; RSA tokens likely involved," by William Jackson, Jun 01, 2011, http://gcn.com/articles/2011/06/01/defense-contractors-l3-lockheed-hacked.aspx accessed 9/23/2013

- Attacks on corporate networks have become commonplace
- Attackers know who is working on what (it's on their webpage!)
- Once they get in, they know what to look for and where

What is Cloud Computing?

Hint: It's not just a website

What is cloud computing?

- Definition from NIST:
  - *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of* ***five essential characteristics, three service models, and four deployment models***

From presentation by Jim Sweeney, GTSI at the Technology Leadership Series 2012 Seminar, January 19, 2012

SPEC INNOVATIONS

Five Essential Characteristics

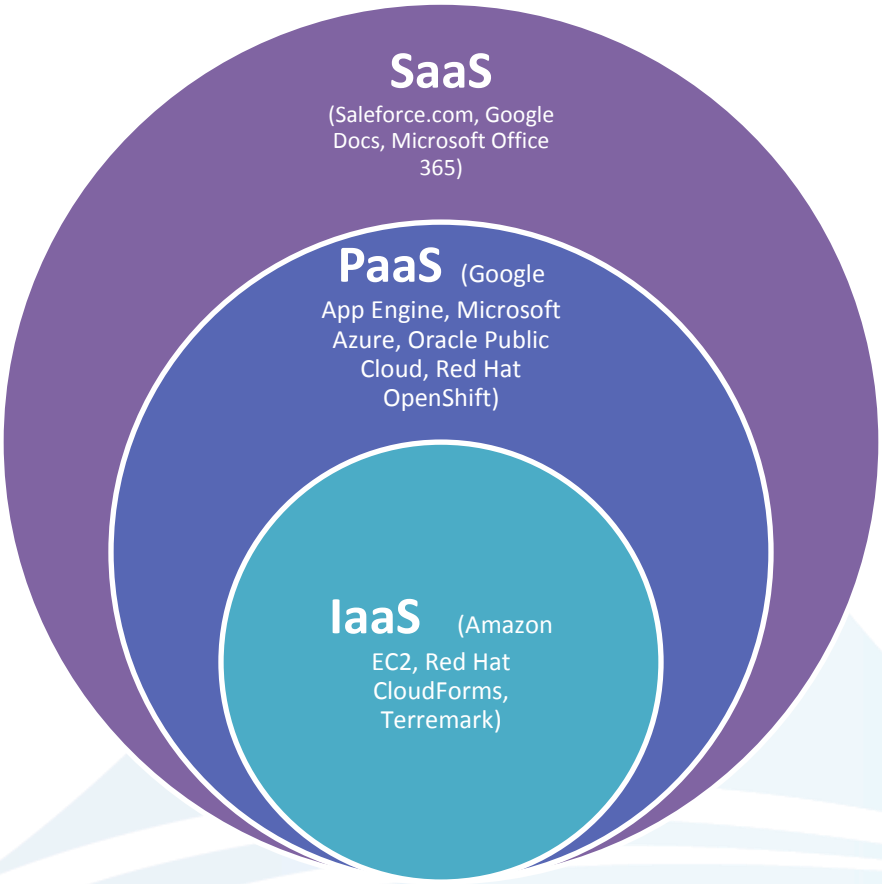
- ***On-demand self-service.*** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- ***Broad network access.*** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- ***Resource pooling.*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- ***Rapid elasticity.*** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- ***Measured Service.*** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

From presentation by Jim Sweeney, GTSI at the Technology Leadership Series 2012 Seminar, January 19, 2012

SPEC INNOVATIONS

Three Service Models

- Software as a Service (SaaS): The end user system
- Platform as a Service (PaaS): Tools and services to create a SaaS Application
- Infrastructure as a Service (IaaS): Full control of the software stack and services



Four Deployment Models

Private cloud
- Operated solely for an organization
- May be managed by the organization or a third party

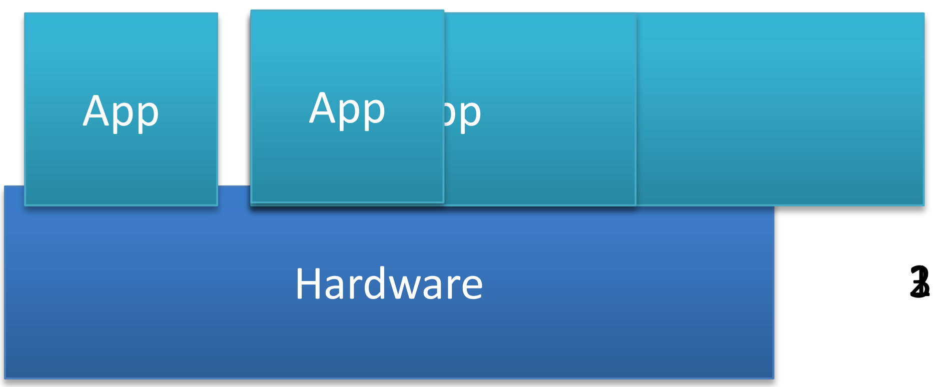
Public cloud
- Available to the general public or a large industry group
- Owned by an organization selling cloud services

Community cloud
- Shared by several organizations
- Managed by the organizations or a third party

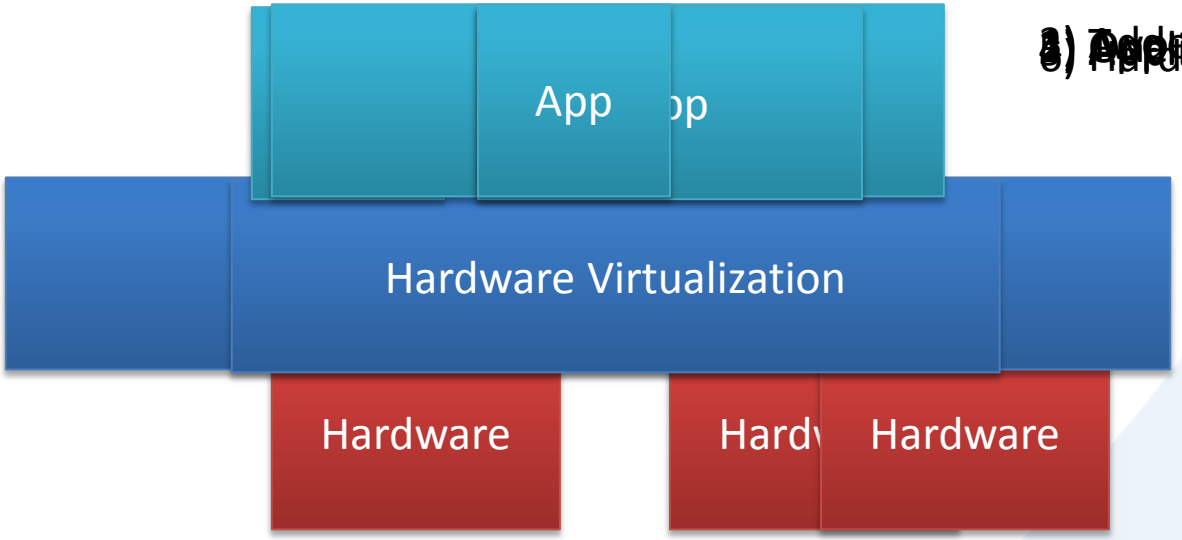
Hybrid cloud
- composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

SPEC INNOVATIONS

Normal Server Deployment

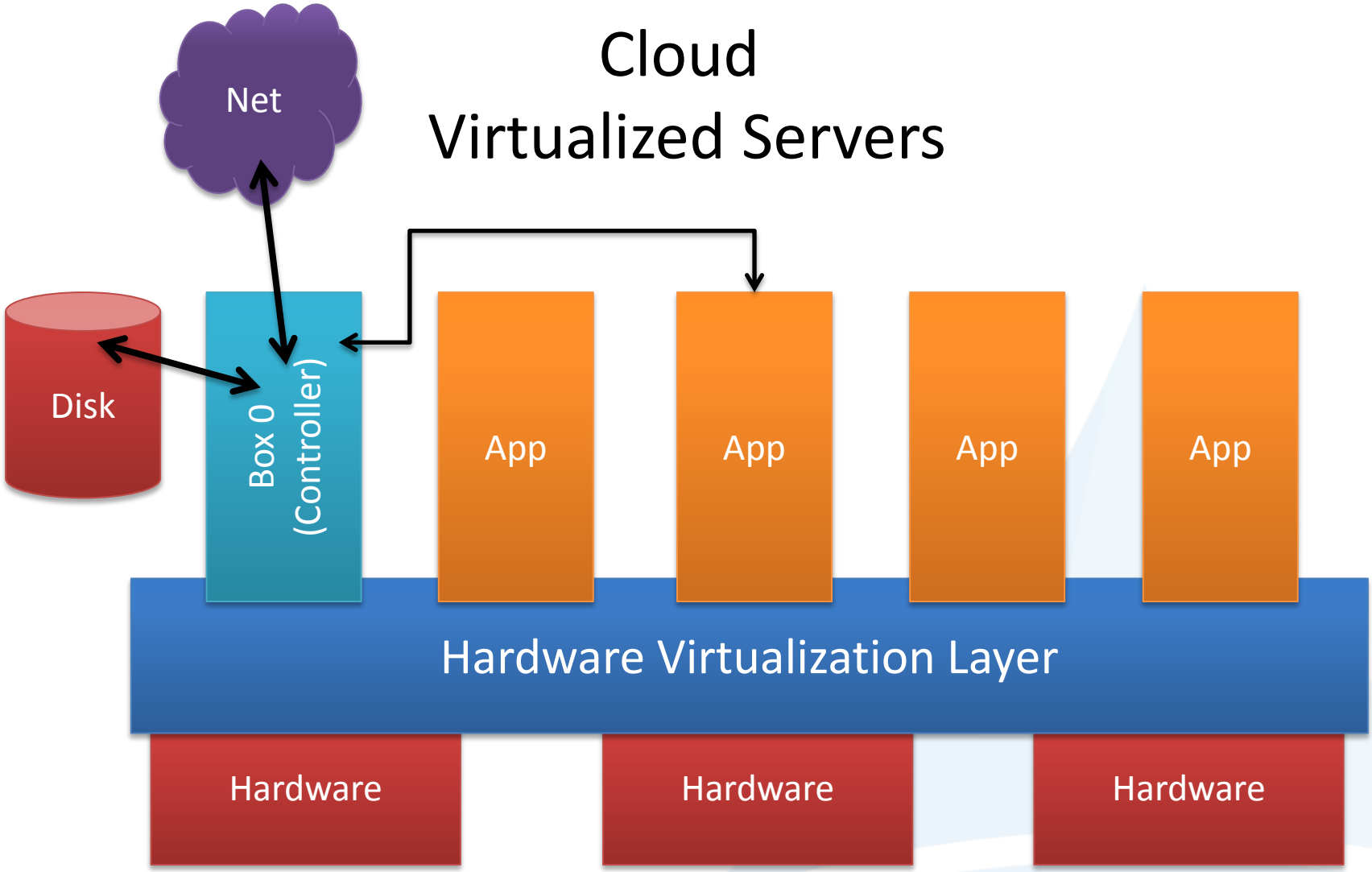


Virtualized Server Deployment



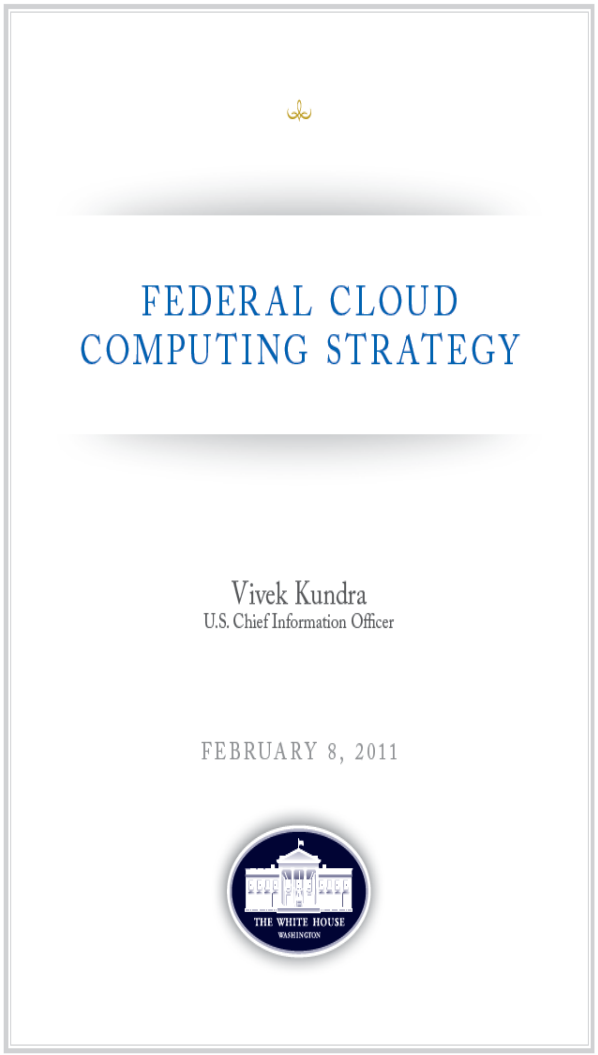
virtualization continues

Cloud
Virtualized Servers



SPEC INNOVATIONS

"Cloud-First" Policy



"The Federal Government's current Information Technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. These inefficiencies negatively impact the Federal Government's ability to serve the American public."

"Cloud computing has the potential to play a major part in addressing these inefficiencies and improving government service delivery. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints."

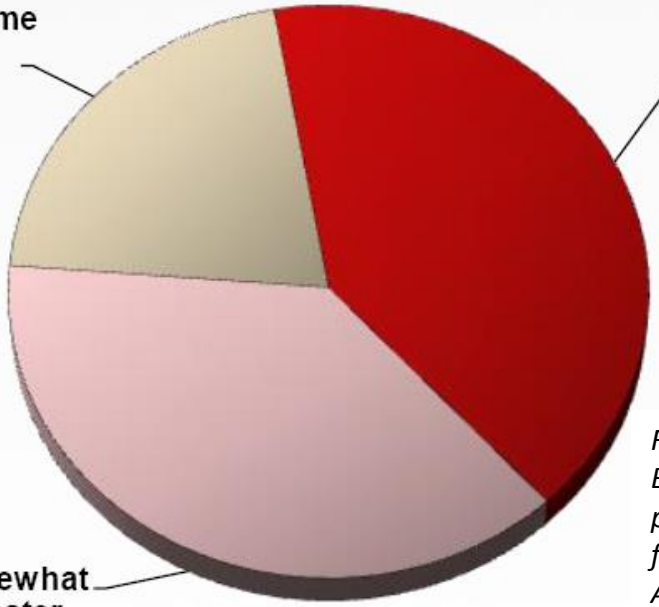
SPEC INNOVATIONS

What Are Key Security Issues?

Who has access to my data?

Cybersecurity concerns are omnipresent

"Compared to two years ago, how concerned are you for cybersecurity threats"



No government agency reports having <u>less</u> concern about cybersecurity threats

Federal agencies (civilian and DOD) are significantly more likely to be concerned about cybersecurity threats

From presentation by James McLeod-Warrick, Beacon Technology Partners, July 25, 2013, as part of a webinar on "Data Security: Moving from Security Worries to Security Solutions." Accessed 9/23/2013

Base = Total Respondents

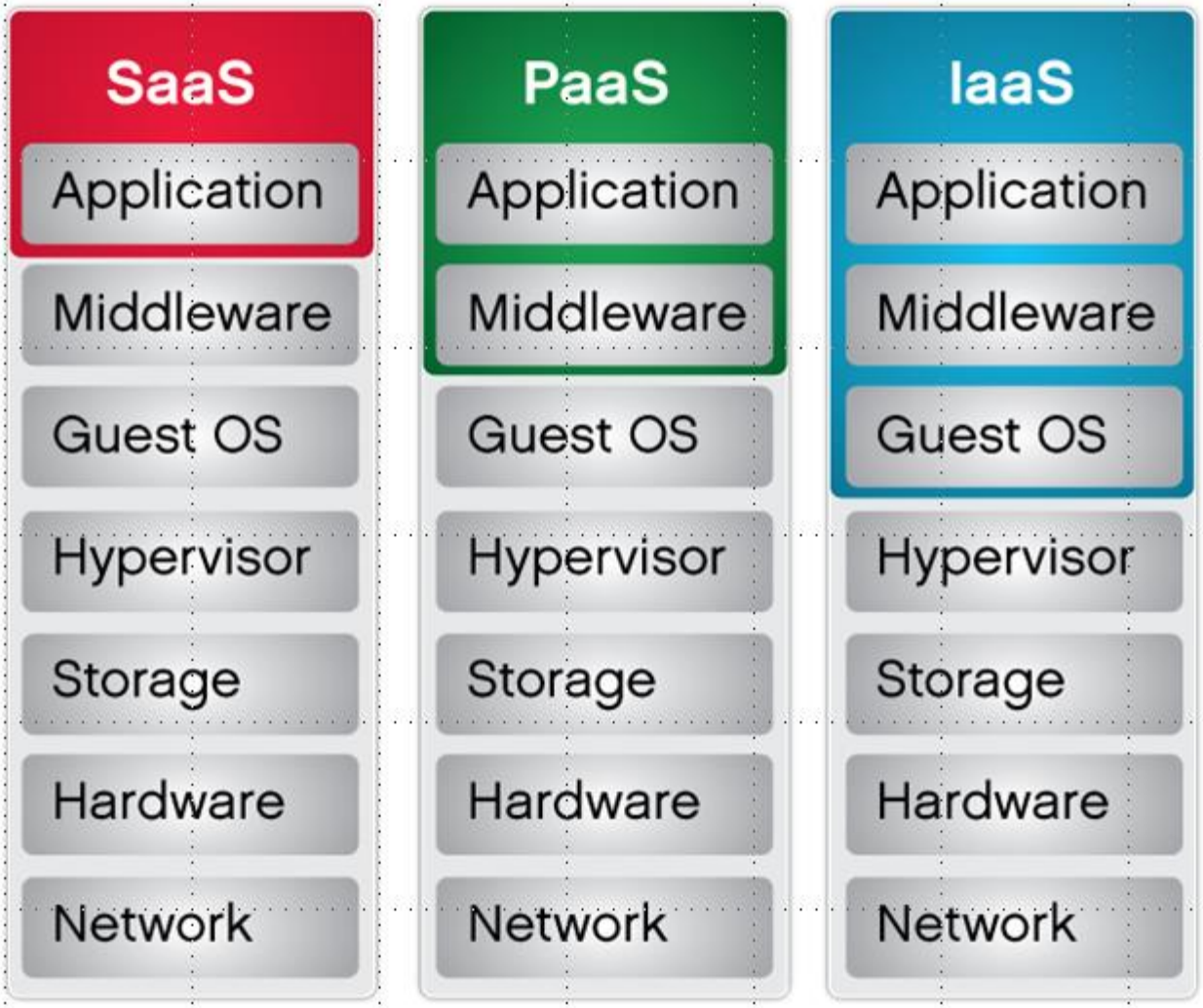
FCW

10. How concerned is your agency or department with threats related to ***<u>cyber-security</u>*** threats compared to two years ago?

GCN

Security Differs Depending on Cloud Type

Security must be addressed at each layer



From presentation by Jim Sweeney, GTSI at the Technology Leadership Series 2012 Seminar, January 19, 2012

TECHNOLOGY LEADERSHIP SERIES 2012

Best Practices for Security in the Cloud

- Security Should be implemented at every layer of the app architecture:
  - Physical Layer
  - Network Layer
  - Data Layer (at-rest and in-transit)
  - Operating System
  - Credential Management
- In the Public IaaS Cloud, this is a shared responsibility:

From presentation by Jim Sweeney, GTSI at the Technology Leadership Series 2012 Seminar, January 19, 2012

Vendor Responsibility	User Responsibility
Facilities	Operating System
Physical Security	Application
Physical Infrastructure	Security Groups
Network Infrastructure	OS Firewalls
Virtualization Infrastructure	Network Configuration
	Account Management
	Application Certifications

What Is FedRAMP?

USG Approach to Cloud Authorization – Risk Based

FedRAMP provides a means to "ensure government use of the cloud is secure and minimizes costs to cloud providers"

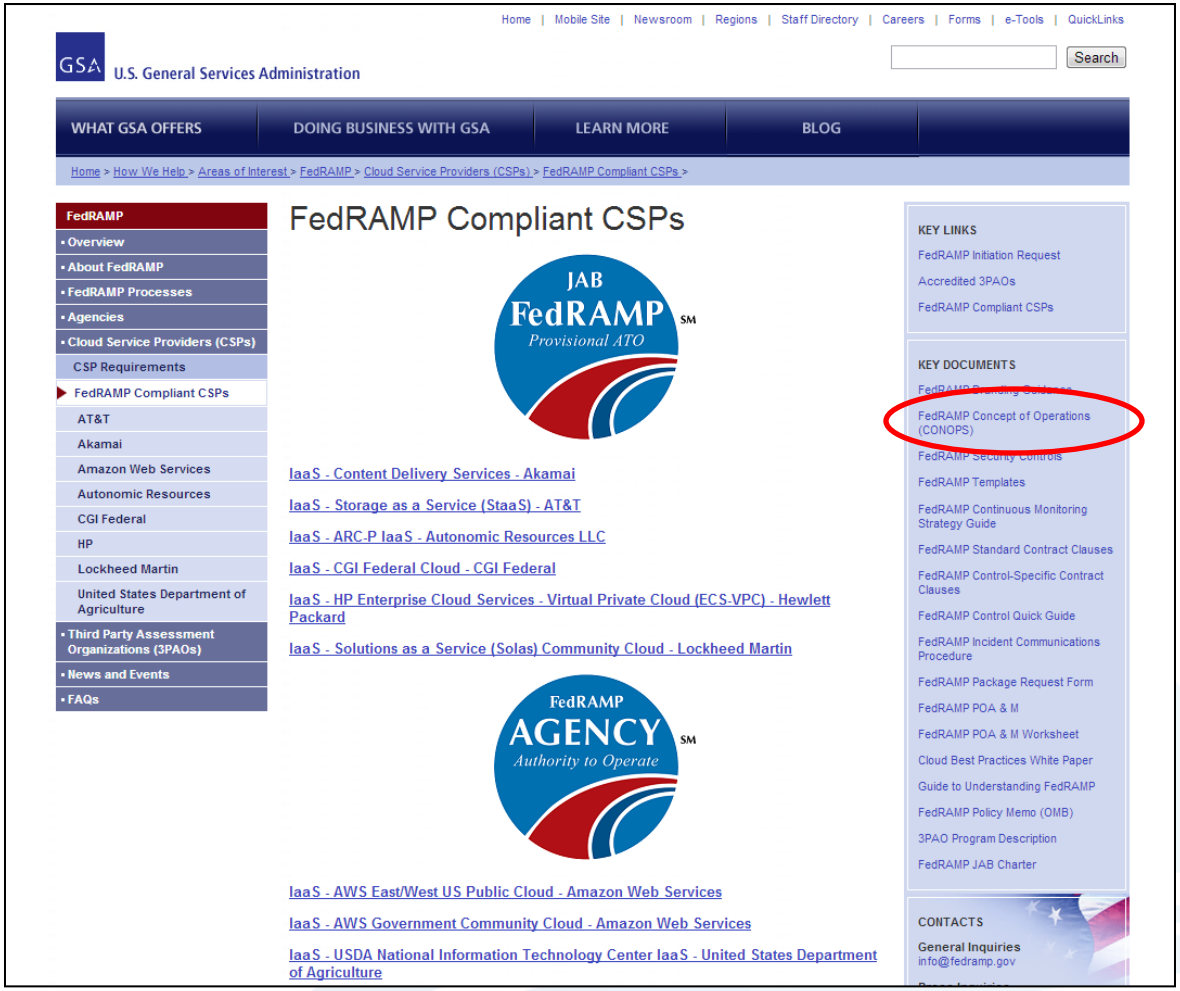
IOC was June 2012

See http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_medium=print-radio&utm_term=fedramp&utm_campaign=shortcuts

SPEC INNOVATIONS

Who Has Been Approved?

- After over one year only a few
- 49 Page CONOPS
- These services are expensive compared to large commercial services



Shifting the Responsibility

- Agency always bears some responsibility for security, but this approach shifts that responsibility to the service provider
- Will commercial applications developers what to bear that responsibility?
  - Only if they pay for it

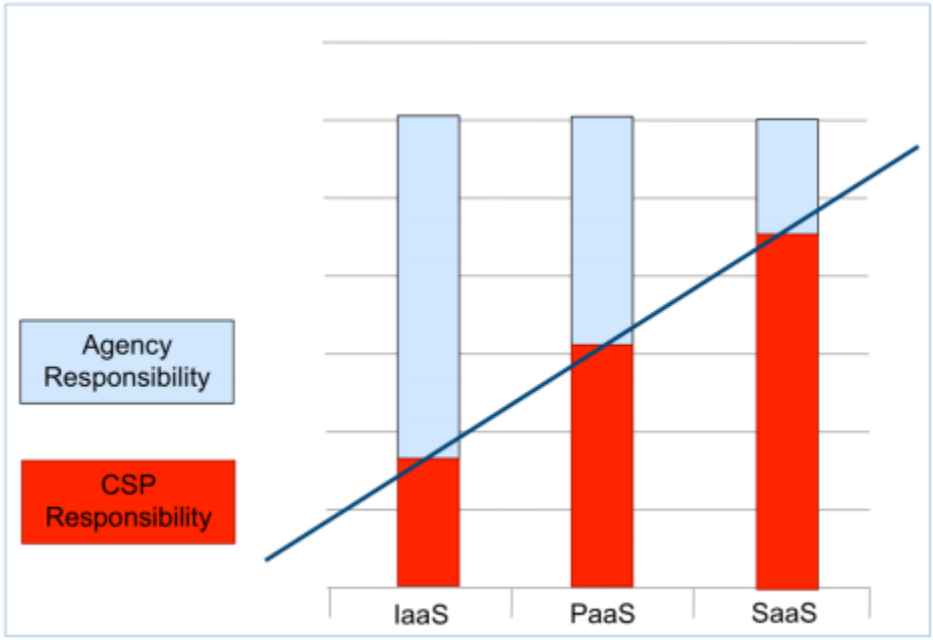


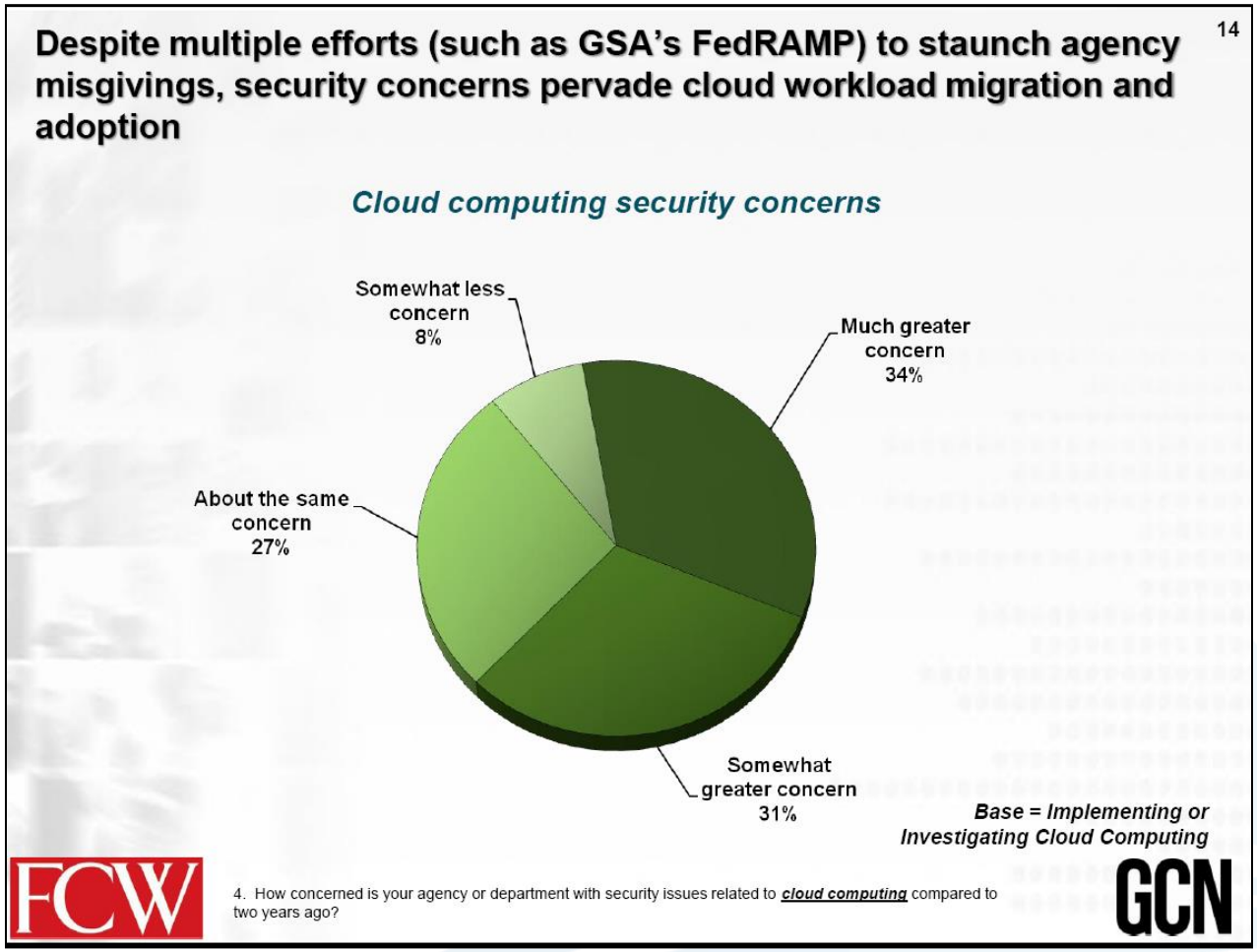
Figure 7-2. Security Control Responsibilities

From FedRAMP CONOPS, accessed 9/23/2013

Are You Still Concerned?

- The answer is Yes!

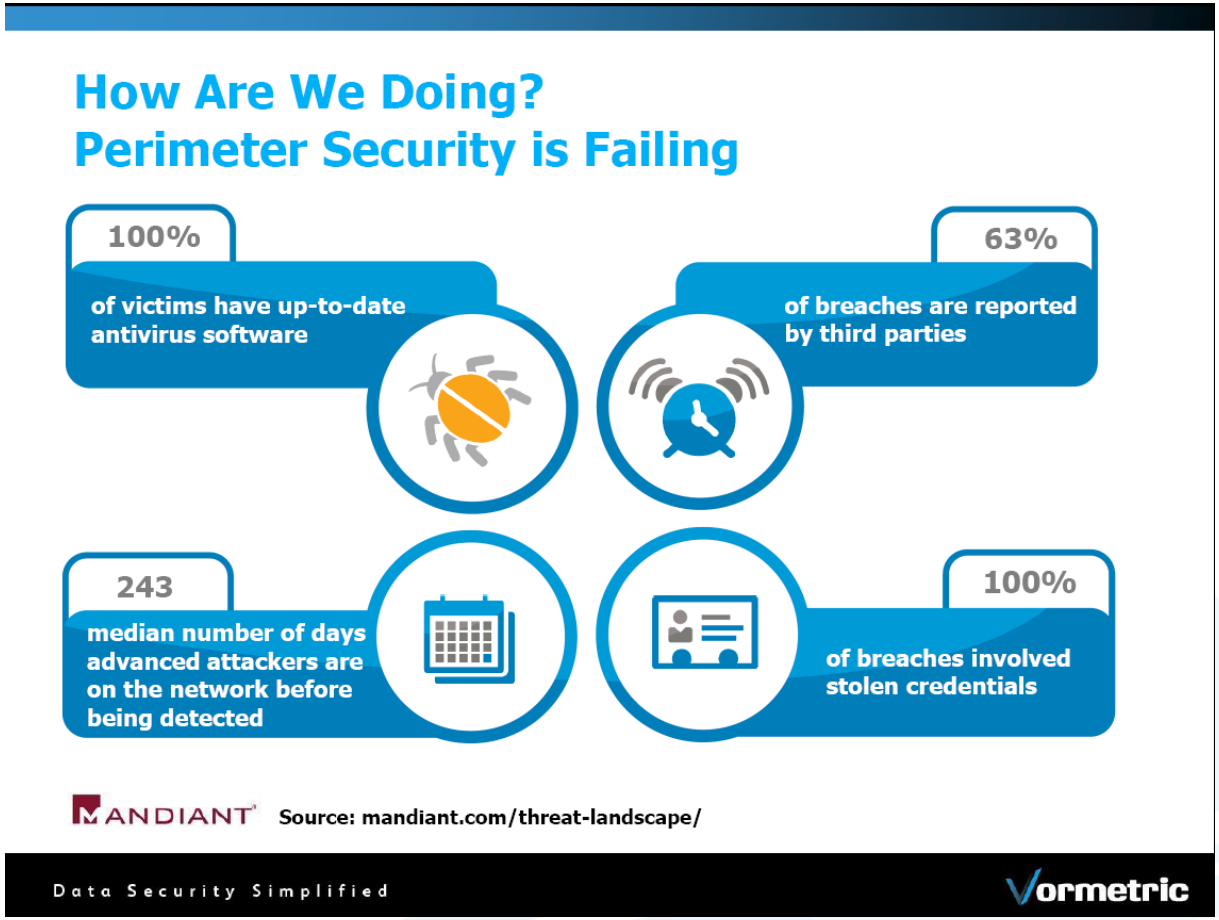
From presentation by James McLeod-Warrick, Beacon Technology Partners, July 25, 2013, as part of a webinar on "Data Security: Moving from Security Worries to Security Solutions." Accessed 9/23/2013



How Are We Trying to Fix the Problem?

How Are We Trying to Fix the Problem?

- Once through the perimeter, it's open access
- We need defense in depth

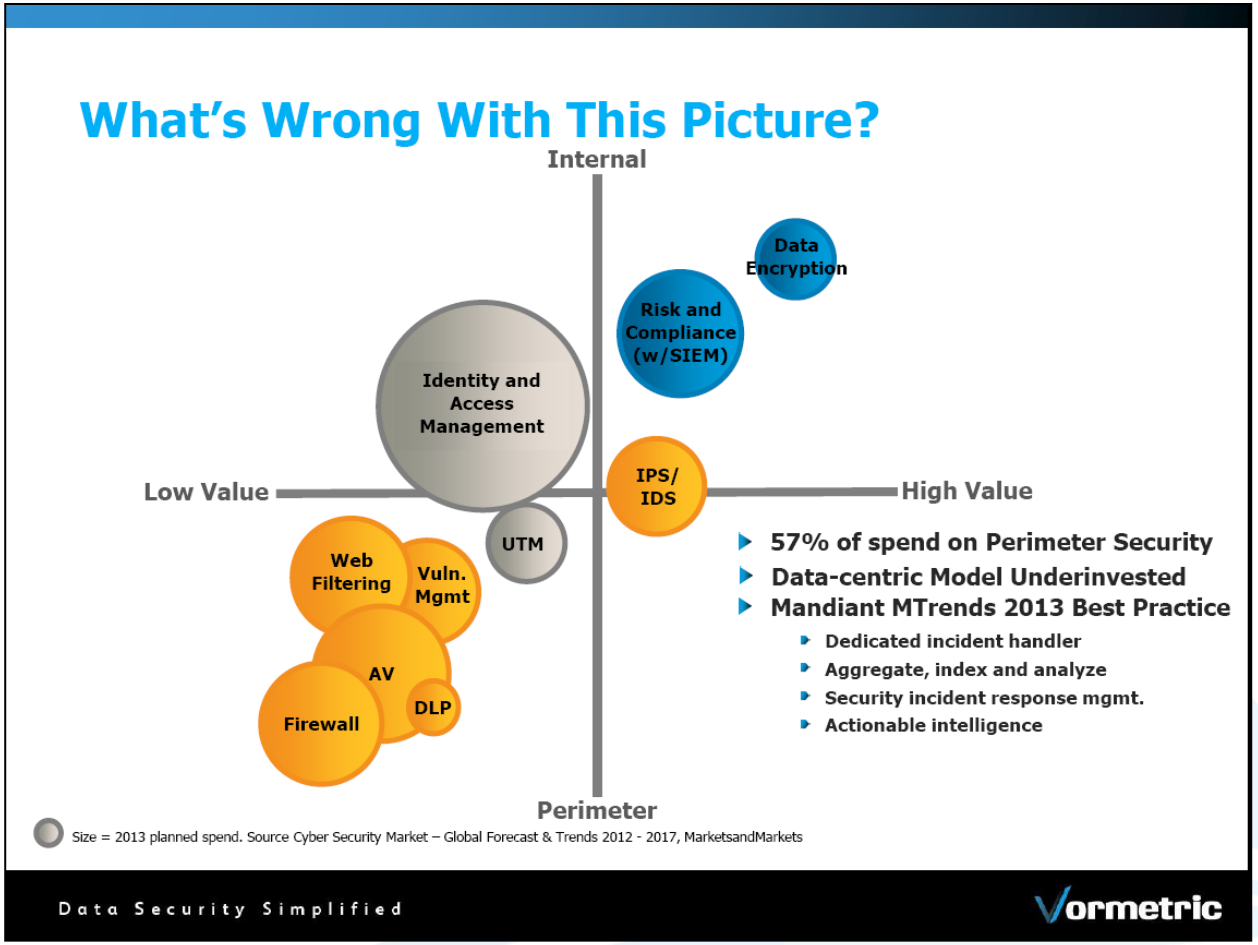


From presentation by Sol Cates, Vormetric, July 25, 2013, as part of a webinar on "Data Security: Moving from Security Worries to Security Solutions." Accessed 9/23/2013

SPEC INNOVATIONS

Where Are We Investing in Security Solutions?

- Heavy emphasis today on firewalls and access controls
- Still working on the perimeter



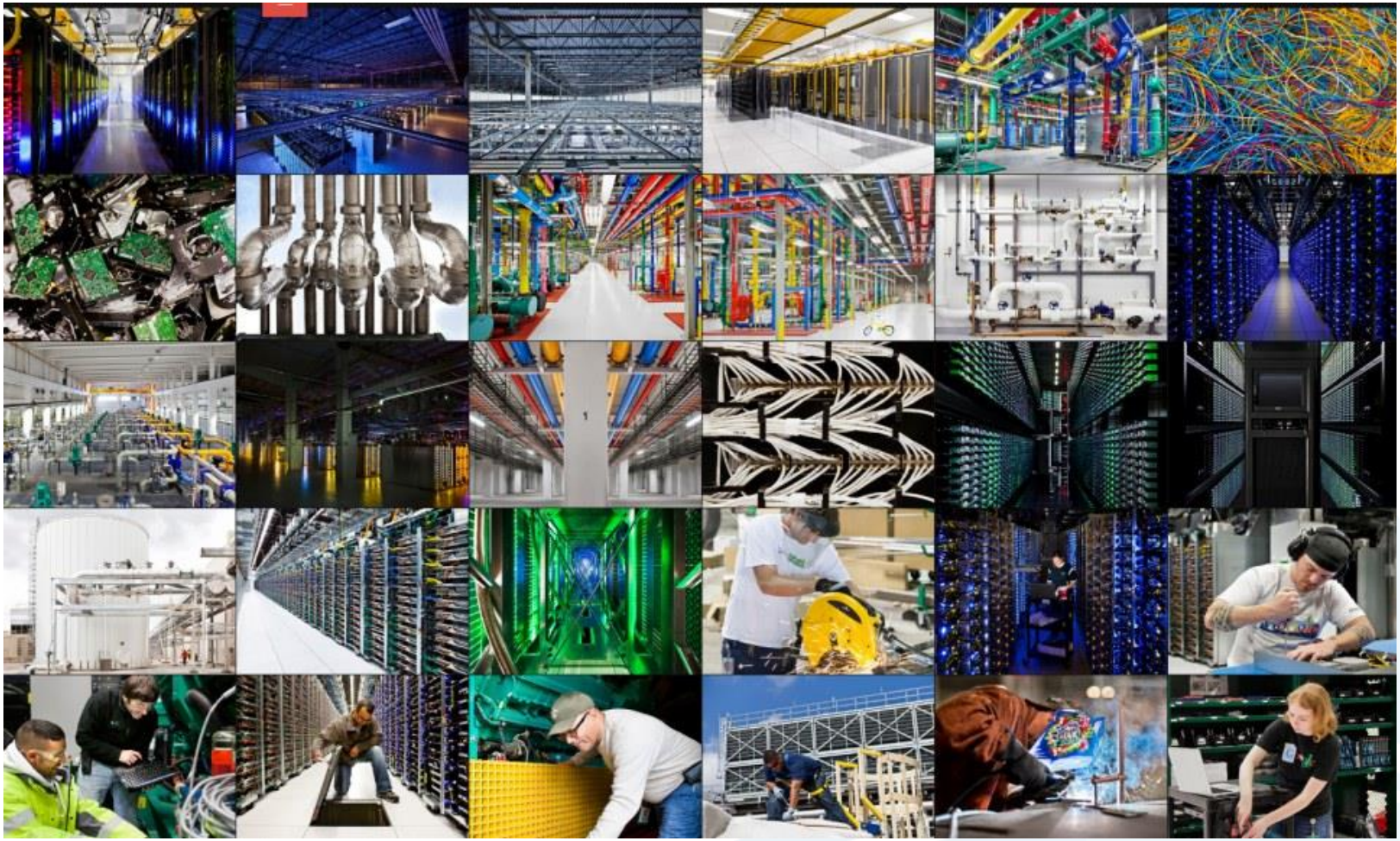
From presentation by Sol Cates, Vormetric, July 25, 2013, as part of a webinar on "Data Security: Moving from Security Worries to Security Solutions." Accessed 9/23/2013

SPEC INNOVATIONS

What Does Google Do?

A leader in cloud computing

Google Data Centers



From http://www.dailymail.co.uk/sciencetech/article-2219188/Inside-Google-pictures-gives-look-8-vast-data-centres.html accessed 9/23/2013

SPEC INNOVATIONS

World-wide Data Centers

Data center locations

We own and operate data centers around the world to keep our products running 24 hours a day, 7 days a week. Find out more about our data center locations, community involvement, and job opportunities in our locations around the world.

Americas

Berkeley County, South Carolina
Council Bluffs, Iowa
Douglas County, Georgia
Quilicura, Chile
Mayes County, Oklahoma
Lenoir, North Carolina
The Dalles, Oregon

Asia

Hong Kong
Singapore
Taiwan

Europe

Hamina, Finland
St Ghislain, Belgium
Dublin, Ireland

Key Google Security Features

- "We build custom servers exclusively for our data centers, never selling or distributing them externally."
- "We've also designed them so they don't include unnecessary hardware or software—reducing the number of potential vulnerabilities."
- "Rather than storing each user's data on a single machine or set of machines, we distribute all data—including our own—across many computers in different locations."
- "We then chunk and replicate the data over multiple systems to avoid a single point of failure. We randomly name these data chunks as an extra measure of security, making them unreadable to the human eye."
- "We rigorously track the location and status of each hard drive in our data centers. We destroy hard drives that have reached the end of their lives in a thorough, multi-step process to prevent access to the data."
- "Our full-time Information Security Team maintains the company's perimeter defense systems, develops security review processes, and builds our customized security infrastructure."
- "At the data centers themselves, we have access controls, guards, video surveillance, and perimeter fencing to physically protect the sites at all times."

From http://www.google.com/about/datacenters/inside/data-security/index.html accessed 9/23/2013

From Interview with Google Apps Security Director

- "Information security is really part of our culture at Google, both in the security group and outside, in all of our engineering culture."
  - **People**: "Do we have the right people in the places that we need to? Do we have the best experts that we can have to do those tasks?"
  - **Processes**: "How do we engineer processes to make it easier for people to do the right thing, that is, the secure thing, than it is to do the wrong thing? and testing those processes."
  - **Tools**: "Do we have the technology to support those processes?"

Sounds like systems engineering?

SPEC INNOVATIONS

From Interview with Google Apps Security Director (continued)

- "For example, one of the benefits that Google has is we have a very homogeneous environment. All of our machines look, basically, the same which allows you to respond to an incident or to a patch in a much more rapid manner when there is a vulnerability out there, as opposed to most organizations today that have a heterogeneous environment with different flavors of different operating systems, different applications running on them, and they have to start running around and figuring out what is going to break."

Google Apps security director discusses compliance within the cloud
Date: Mar 11, 2011. In this exclusive video from RSA Conference 2011, Google Apps Security Director, Eran Feigenbaum discusses compliance within the cloud, including his thoughts on emerging cloud security standards. From http://searchcloudsecurity.techtarget.com/video/Google-Apps-security-director-discusses-compliance-within-the-cloud?videoId=2f481ff42a6ae210VgnVCM1000000d01c80aRCRD accessed 9/23/2013

SPEC INNOVATIONS

Has Google Ever Had a Problem?

- “Google has confirmed that a software bug exposed documents thought to be privately stored in the Internet giant's online Docs application service.”
- “The problem was fixed by the weekend and is believed to have affected only .05 percent of the digital documents at a Google Docs service that provides text-handling programs as services on the Internet.”
- "We've identified and fixed a bug where a very small percentage of users shared some of their documents inadvertently," Google Docs Product Manager Jennifer Mazzon wrote in a message at the firm's website on Saturday.”

From “Google software bug shared private online documents,” March 9, 2009, http://www.google.com/hostednews/afp/article/ALeqM5iijbwg-AdroJ-F8buwfBpuLzLhJA accessed 9/23/2013.

SPEC INNOVATIONS

Summary

How Secure is the Cloud?

- We are using Google App Engine for our SaaS application development:
  - Proven Reliability: Google App Engine is one of the most secure enterprise services in the world
  - Multiple layers of physical and virtual security
  - Safer than most internal networks: With multiple layers of firewalls, sandboxed code, and software protection Google App Engine is more secure than most company networks

SPEC INNOVATIONS

Cloud Computing Security Bottom-Line

- FedRAMP will help, but it's no panacea
- Commercial cloud providers, such as Google, have a vested interest in protecting our data
- It's good enough for the financial and medical communities
- Is it good enough for us?

SPEC INNOVATIONS